多変数多項式環を用いたNTRU暗号の拡張 (Computer Algebra : Design of Algorithms, Implementations and Applications)

AUTHOR(S):

小柴, 薫居; 井上, 秀太郎; 和田, 雅美; 森田, 昌宏

数理解析研究所講究録
第1815巻 2012年 79-89

多変数多項式環を用いたNTRU暗号の拡張

小柴薫居
Masaori Koshiba
東京理科大学大学院理学研究科数理情報科学専攻
DEPARTMENT OF MATHEMATICAL INFORMATION SCIENCE,
GRADUATE SCHOOL OF SCIENCE,
TOKYO UNIVERSITY OF SCIENCE

井上秀太郎
Shutaro Inoue
東京理科大学理学部数理情報科学科
DEPARTMENT OF MATHEMATICAL INFORMATION SCIENCE,
TOKYO UNIVERSITY OF SCIENCE

和田雅美
Masami Wada
東京理科大学理学部数理情報科学科
DEPARTMENT OF MATHEMATICAL INFORMATION SCIENCE,
TOKYO UNIVERSITY OF SCIENCE

森田昌宏
Masahiro Morita
東京理科大学理学部数理情報科学科
DEPARTMENT OF MATHEMATICAL INFORMATION SCIENCE,
TOKYO UNIVERSITY OF SCIENCE

Abstract

NTRU[1] はCRYPTO 96で発表された公開鍵暗号で, 1変数多項式環上に構成されたものである. 既存の暗号に対して暗号化にかかる計算量が少ないことが知られている. NTRUに対する攻撃方法として総当たり攻撃やLattice Attack[2]が知られている. 本研究ではNTRUを1変数多項式環から多変数多項式環に拡張し, 新しい公開鍵暗号化方式 (MTRU) を構築した. またRisa/Asirを用いてNTRUとMTRUを実装し実行時間, 安全性を比較した.

1 はじめに

NTRU[1] (N-th Degree Truncated Polynomial Ring) は 1 変数多項式環上で構成された公開鍵暗号である. 暗号化に必要な計算量は $O(N^2)$(FFT を用いれば $O(N \log N)$) である. RSA は暗号化に $O(N^3)$ かかるので RSA より早いとされている. 派生系として CTRU, MaTRU, GB-TRU などが提案されている. また NTRUSign[3] として NTRU 格子を用いたデジタル署名方式も提案されている.

NTRU における暗号化関数 f は, n を自然数, $p, q(p < q)$ を素数, H を公開鍵, R をランダムな多項式, $*$ を $Z_q[x]/I$ における積として以下で表される.

$$\begin{array}{rccc} f: & Z_p[x]/(x^n-1) & \rightarrow & Z_q[x]/(x^n-1) \\ & \cup & & \cup \\ & M & \mapsto & pH * R + M \end{array}$$

NTRU に対する攻撃方法として総当たり攻撃や Meet-In-The-Middle Attack, Lattice Attack[2] が知られている. NTRU においてこれらの攻撃に対する安全性を高めるためには次数 n を上げる他に方法はない.

本研究では NTRU を 1 変数多項式環から多変数多項式環に拡張し, 新しい公開鍵暗号化方式を構築した. これを MTRU(Multivariable Truncated Polynomial Ring) と呼ぶこととする. さらに数式処理システム Risa/Asir を用いて NTRU と MTRU をそれぞれ実装し, 実行時間, 安全性を比較検討した.

MTRU における暗号化関数 f は, m を自然数, $p, q(p < q)$ を素数, P, Q をイデアル, $P_1, \cdots, P_m$ を P の生成元, H を公開鍵, $R_1, \cdots, R_m$ をランダムな多項式, $\circledast$ を $Z_q[x_1, \cdots, x_m]/Q$ における積として以下で表す.

$$\begin{array}{rccc} f: & Z_p[x_1, \cdots, x_m]/P & \rightarrow & Z_q[x_1, \cdots, x_m]/Q \\ & \cup & & \cup \\ & M & \mapsto & H \circledast \sum_{i=1}^{m} P_i \circledast R_i + M \end{array}$$

MTRU では多変数多項式環を用いることにより, イデアル P の生成元の次数を大きくするだけでなく, 変数 m を増やすことにより安全性を高めることが可能である. また NTRU では平文の集合と暗号文の集合は係数体が異なるだけであったが, MTRU では法となるイデアルも異なるものとした. このことにより暗号化関数にランダムな多項式が増え, 暗号文への総当たり攻撃に対する安全性が向上した.

2 NTRU

本章では NTRU についてまとめる. 以降, 本章では 1 変数多項式環 R を $\mathbb{Z}[x]$, イデアル I を $\langle x^n - 1 \rangle \subset \mathbb{Z}[x]$ とし, 剰余環 R/I の元である n 次多項式 F を以下で表記する.

$$F = \sum_{i=0}^{n} F_i x^i$$

係数 $F_0, \cdots, F_n$ のうち d_1 個が 1, d_2 個が -1, 残りが 0 である多項式の集合を $\mathcal{L}(d_1, d_2) \subset R/I$ とする.

2.1 鍵生成

p, q を $p \ll q$ なる互いに異なる自然数とする. $n/2$ 未満の自然数 d_L, d_G を決定する. $\mathbb{Z}_p[x]/I$ と $\mathbb{Z}_q[x]/I$ 上で逆元 F_p^{-1}, F_q^{-1} をもつ多項式 $F \in \mathcal{L}(d_L, d_L - 1)$ は十分存在するので, これを決定する.

$$F * F_p^{-1} \equiv 1 \pmod{p} \pmod{I}$$
$$F * F_q^{-1} \equiv 1 \pmod{q} \pmod{I}$$

次に $G \in \mathcal{L}(d_G, d_G)$ をランダムに選ぶ. この G と F_q^{-1} から H を生成する.

$$H \equiv G * F_q^{-1} \pmod{q} \pmod{I}$$

公開鍵を $\{p, q, H, I\}$, 秘密鍵を $\{F, F_p^{-1}\}$ とする.

2.2 暗号化

平文を $M \in \mathbb{Z}_p[x]/I$ とする. $R \in \mathcal{L}(d_R, d_R)\}(d_R$ は $n/2$ 未満の自然数) をランダムに選び, 以下の式で暗号文 C を生成する.

$$C \equiv p \cdot H * R + M \pmod{q} \pmod{I}$$

2.3 復号

暗号文 C に対し, 秘密鍵 F によって A を求め

$$A \equiv C * F \pmod{q} \pmod{I}$$

F の $Z_p[x]/I$ における逆元 F_p^{-1} によって復号文 M' を求める.

$$M' \equiv A * F_p^{-1} \pmod{p} \pmod{I}$$

2.4 復号条件

パラメータ p, q, d_L, d_G, d_R の取り方と, 平文の係数等によっては復号できない場合がある.

定理 1 (復号条件)
$|F|_\infty$ を次のように定義し

$$|F|_\infty \equiv \max_{0 \leqslant i \leqslant n} \{F_i\} - \min_{0 \leqslant i \leqslant n} \{F_i\}$$

復号文が平文に一致するための必要条件は以下である.

$$|p \cdot G * R + F * M|_\infty \leqslant q$$

証明
復号過程において

$$\begin{aligned}
A &\equiv C * F && \pmod{q} \pmod{I} \\
&\equiv p \cdot F * H * R + F * M && \pmod{q} \pmod{I} \\
&\equiv p \cdot F * F_q^{-1} * G * R + F * M && \pmod{q} \pmod{I} \\
&\equiv p \cdot G * R + F * M && \pmod{q} \pmod{I}
\end{aligned}$$

である. ここで $|p \cdot G * R + F * M|_\infty \leqslant q$ ならば, R/I 上で

$$A = p \cdot G * R + F * M$$

である. よって,

$$\begin{aligned} M' &\equiv A * F_p^{-1} && (\mathrm{mod}\ p)(\mathrm{mod}\ I) \\ &\equiv p \cdot F_p^{-1} * G * R + F_p^{-1} * F * M && (\mathrm{mod}\ p)(\mathrm{mod}\ I) \\ &\equiv M && (\mathrm{mod}\ p)(\mathrm{mod}\ I) \end{aligned}$$

であるので復号文は平文と一致する. □

3 MTRU

3.1 準備

記号の定義を以下とする.

$$\begin{aligned} \bar{x} &:= x_1, \cdots, x_m \\ k &: \text{体} \\ R &:= k[x_1, \cdots, x_m] \\ I &:= \langle f_1, \cdots, f_s | f_i \in R \rangle \\ \sqrt{I} &:= \{ f | \exists n, f^n \in I \} \\ \mathbf{V}(I) &:= \{ (a_1, \cdots, a_n) \in k^n | \forall f \in I, f(a_1, \cdots, a_m) = 0 \} \\ V &:= \text{多様体} \\ \mathbf{I}(V) &:= \{ f \in R | \forall x \in V, f(x) = 0 \} \\ \mathrm{LT}(f) &:= f \text{ の先頭項} \\ \mathrm{multideg}(f) &: f \text{ の多重次数} \\ \mathcal{L}_I(d_1, d_2) &:= \{ \text{ 係数のうち } d_1 \text{個が } 1, d_2 \text{個が } -1, \text{残りが } 0 \text{ である } R/I \text{ の元 } \} \\ \dim(X) &: \text{線形空間 } X \text{ の次元} \end{aligned}$$

定理 2
剰余環 R/I の元 f の逆元 f^{-1} が存在することの必要十分条件は以下である. z を $x_1, \cdots, x_n$ と異なる変数とする. 単項式順序を $z > x_1 > \cdots > x_n$ の辞書式順序とする. このときイデアル $J = \langle f * z - 1, f_1, \cdots, f_s \rangle \subset k[\bar{x}, z]$ の簡約グレブナ基底 G に先頭項が z となる多項式が含まれる.
この多項式を $z - h$ とすると $h = f^{-1}$ である.

証明
(必要性の証明) J の簡約グレブナ基底に $z - h$ が含まれるとき, $\mathbf{V}(J) = \mathbf{V}(G)$ であるから $z - h = 0$ より $z = h$, これを $f * z - 1 = 0$ に代入して $f * h = 1$ であるから f の逆元は存在し $h = f^{-1}$ である.
(十分性の証明) J の簡約グレブナ基底を $G = \{g_1, \cdots, g_u\}$ とすると

$$\langle \mathrm{LT}(J) \rangle \ = \ \langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_u) \rangle$$

である. よって, ある i により $\mathrm{LT}(f * z - 1)$ を $\mathrm{LT}(g_i)$ が割り切る.
以下 $\mathrm{LT}(f)$ が I の簡約グレブナ基底で簡約できないことから $\mathrm{LT}(g_i) = z$ を示す. I は J から z を消去したイデアルだから消去定理より $G_z = G \cap k[\bar{x}]$ は J の簡約グレブナ基底である.

$f \in R/I$ であるので,

$$\mathrm{LT}(f) < \min\{\mathrm{LT}(g) \mid g \in G_z\}$$

よって変数順序を $z > x_1 > \cdots > x_n$ とし, 単項式順序を辞書式順序としているので $\mathrm{LT}(f)$ は $\mathrm{LT}(g_i)$ で割れない. よって $\mathrm{LT}(g_i) = z$ に他ならないので示された. □

系 3
定理 2 と同じ条件の元で, 剰余環 R/I の元 f の逆元 f^{-1} が存在することの必要十分条件は以下である.

$$\langle g_1, \cdots, g_u, f \rangle = \{1\}$$

証明
逆元 f が存在するならば,

$$\begin{aligned} & f * f^{-1} \equiv 1 \pmod{I} \\ \Leftrightarrow & f * f^{-1} = a_1 * g_1 + \cdots + a_u * g_u + 1 \\ \Leftrightarrow & f * f^{-1} - a_1 * g_1 - \cdots - a_u * g_u = 1 \\ \Leftrightarrow & 1 \in \langle g_1, \cdots, g_u, f \rangle \end{aligned}$$

よって $\langle g_1, \cdots, g_u, f \rangle = \{1\}$.
逆に $\langle g_1, \cdots, g_u, f \rangle = \{1\}$ ならば $f * h \equiv 1 \pmod{I}$ なる元が存在し, これは逆元に他ならないので示された. □

3.2 鍵生成

変数の数 m, 互いに異なる自然数 $p, q (p \ll q)$, 2 つのグレブナ基底 P, Q を決定する. この選び方については 3.6 にて詳しく述べる. l_p, l_q を P, Q の生成元の数とする. $R/P, R/Q$ を線形空間としてみたときの次元をそれぞれ以下とする.

$$\begin{aligned} n_p &= \dim(R/P) \\ n_q &= \dim(R/Q) \end{aligned}$$

$n_p/2$ 未満の自然数 d_F, d_G を決定する. 多項式 $F \in \mathcal{L}_P(d_F, d_F - 1)$ をランダムに選び, 定理 2 により $\mathbb{Z}_p[\bar{x}]/P, \mathbb{Z}_q[\bar{x}]/Q$ 上に逆元 F_P^{-1}, F_Q^{-1} を持つか調べる. これらの逆元 F_P^{-1}, F_Q^{-1} が両方存在する多項式 F を選ぶ.

$$\begin{aligned} F \circledast F_P^{-1} &\equiv 1 \pmod{p} \pmod{P} \\ F \circledast F_Q^{-1} &\equiv 1 \pmod{q} \pmod{Q} \end{aligned}$$

またこのことに関しては??にて詳しく述べる.
次に $G \in \mathcal{L}_P(d_G, d_G)$ をランダムに選ぶ. この G と F_Q^{-1} から H を生成する.

$$H \equiv G \circledast F_Q^{-1} \pmod{q} \pmod{Q}$$

公開鍵を $\{q, H, P, Q\}$, 秘密鍵を $\{F, F_P^{-1}\}$ とする.

3.3 暗号化

平文を $M \in \mathbb{Z}_p[\bar{x}]/P$ とする. $R_i \in \mathcal{L}_P(d_R, d_R)$ をランダムに選び C を生成する.

$$C \equiv H \circledast \sum_{i=0}^{l_p}(P_i \circledast R_i) + M \quad (\mathrm{mod}\ q)(\mathrm{mod}\ Q)$$

3.4 復号

まず暗号文 C と秘密鍵 F から A を求め,

$$A \equiv C \circledast F \quad (\mathrm{mod}\ q)(\mathrm{mod}\ Q)$$

生成した A より復号文 M' を求める.

$$M' \equiv A \circledast F_P^{-1} \quad (\mathrm{mod}\ p)(\mathrm{mod}\ P)$$

3.5 復号条件

定理 4 (復号条件)
復号文が平文と一致する必要条件は以下である.

$$\left| G \circledast \sum_{i=0}^{l_p} \circledast R_i + F \circledast M \right|_\infty \leqslant q$$

証明
復号の過程において

$$\begin{aligned}
A &\equiv C \circledast F \quad (\mathrm{mod}\ q)(\mathrm{mod}\ Q) \\
&\equiv F \circledast H \circledast \sum_{i=0}^{l_p}(P_i \circledast R_i) + F \circledast M \quad (\mathrm{mod}\ q)(\mathrm{mod}\ Q) \\
&\equiv F * F_Q^{-1} \circledast G \circledast \sum_{i=0}^{l_p}(P_i \circledast R_i) + F \circledast M \quad (\mathrm{mod}\ q)(\mathrm{mod}\ Q) \\
&\equiv G \circledast \sum_{i=0}^{l_p}(P_i \circledast R_i) + F \circledast M \quad (\mathrm{mod}\ q)(\mathrm{mod}\ Q)
\end{aligned}$$

となり, P はグレブナ基底なので剰余をとれば $\sum_{i=0}^{l_p}(P_i \circledast R_i) = 0$ より

$$\begin{aligned}
M' &\equiv A \circledast F_P^{-1} \quad (\mathrm{mod}\ p)(\mathrm{mod}\ P) \\
&\equiv F_P^{-1} \circledast G \circledast \sum_{i=0}^{l_p}(P_i \circledast R_i) + F_P^{-1} \circledast F \circledast M \quad (\mathrm{mod}\ p)(\mathrm{mod}\ P) \\
&\equiv M \quad (\mathrm{mod}\ p)(\mathrm{mod}\ P)
\end{aligned}$$

よって, 復号文に平文は一致する. □

3.6 グレブナ基底 P, Q の選び方

3.2 におけるグレブナ基底 P, Q が満たすべき条件は以下である.

1. $\{R/P$ を線形空間としてみたときの基底 $\} \subset \{R/Q$ を線形空間としてみたときの基底 $\}$
2. $\exists f \in P, \forall g \in Q, g \neq 0 \pmod{f}$

条件 1 を満たしていない場合, 平文 M を R/P にとるので暗号化の過程で Q で剰余をとったときに平文の情報が失われてしまう.
条件 2 を満たしていない場合, $C \equiv M \pmod{q} \pmod{P}$ となってしまい簡単に解読されてしまう.

3.7 2変数の場合の例

2 変数の場合の MTRU の具体例をあげる. $\bar{x} = \{x, y\}$, 辞書式順序を採用し, グレブナ基底を $P = \langle x^3 - 1, y^3 - 1\rangle, Q = \langle x^7 - 1, y^7 - 1\rangle$, パラメータを $\{p, q, d_F, d_G, d_R\} = \{3, 89, 3, 1, 1\}$ とした.

$$
\begin{aligned}
F =& x^2 + x + y - xy - 1 \\
F_P^{-1} =& -x - x^2 - y - 2xy - 2y^2 - 2xy^2 - 2x^2y^2 \\
F_Q^{-1} =& -75 - 33x - 34x^2 - 33x^3 - 76x^4 - 72x^5 - 32x^6 - 85y - 54xy - 51x^2y - 15x^3y - 20x^4y \\
& - 31x^5y - 11x^6y - 72y^2 - 11xy^2 - 80x^2y^2 - 55x^3y^2 - 51x^4y^2 - 28x^5y^2 - 59x^6y^2 - 6y^3 \\
& - 54xy^3 - 40x^2y^3 - 69x^3y^3 - 16x^4y^3 - 62x^5y^3 - 20x^6y^3 - y^4 - 68xy^4 - 55x^2y^4 \\
& - 63x^3y^4 - 65x^4y^4 - 85x^5y^4 - 19x^6y^4 - 47y^5 - 51xy^5 - 85x^2y^5 - 55x^3y^5 - 53x^4y^5 \\
& - 39x^5y^5 - 26x^6y^5 - 70y^6 - 85xy^6 - 11x^2y^6 - 66x^3y^6 - 75x^4y^6 - 38x^5y^6 - 11x^6y^6 \\
G =& -y + 1 \\
H =& 84 + 52x + 66x^2 + 33x^3 + 88x^4 + 55x^5 + 68x^6 + 79y + 68xy + 72x^2y + 18x^3y + 56x^4y + 41x^5y \\
& + 21x^6y + 13y^2 + 43xy^2 + 60x^2y^2 + 49x^3y^2 + 58x^4y^2 + 3x^5y^2 + 41x^6y^2 + 66y^3 + 46xy^3 \\
& + 40x^2y^3 + 75x^3y^3 + 35x^4y^3 + 55x^5y^3 + 39x^6y^3 + 5y^4 + 75xy^4 + 74x^2y^4 + 6x^3y^4 + 40x^4y^4 \\
& + 66x^5y^4 + x^6y^4 + 43y^5 + 17xy^5 + 59x^2y^5 + 8x^3y^5 + 12x^4y^5 + 46x^5y^5 + 82x^6y^5 + 66y^6 + 55xy^6 \\
& + 74x^2y^6 + 78x^3y^6 + 67x^4y^6 + x^5y^6 + 15x^6y^6 \\
R_1 =& -x + 1 \\
R_2 =& x - 1 \\
M =& x^2 + xy - y + 1 \\
C =& 52 + 75x + 15x^2 + 84x^3 + 23x^4 + 77x^5 + 32x^6 + 76y + 12xy + 27x^2y + 20x^3y + 74x^4y + 59x^5y \\
& + 88x^6y + 47y^2 + 45xy^2 + 19x^2y^2 + 57x^3y^2 + 41x^4y^2 + 83x^5y^2 + 64x^6y^2 + 33y^3 + 52xy^3 \\
& + 59x^2y^3 + 60x^3y^3 + 14x^4y^3 + 27x^5y^3 + 22x^6y^3 + 65y^4 + 37xy^4 + 20x^2y^4 + 58x^3y^4 + 32x^4y^4 \\
& + 14x^5y^4 + 41x^6y^4 + 32y^5 + 4xy^5 + 19x^2y^5 + 61x^3y^5 + 54x^4y^5 + 8x^5y^5 + 51y^6 + 43xy^6 \\
& + 20x^2y^6 + 16x^3y^6 + 29x^4y^6 + 88x^5y^6 + 20x^6y^6
\end{aligned}
$$

4 安全性

4.1 総当たり攻撃

4.1.1 NTRU

NTRU[1] によれば, 公開鍵に対して H, q, Q は既知であるので G を総当たりすれば F_q^{-1} を求まり, F_q^{-1} より秘密鍵 F を求めることが可能である. よって $\mathcal{L}(d_G, d_G)$ を総当たりすればよい. つまり公開鍵の安全性 (KeySecurity) は

$$\begin{aligned}(\text{KeySecurity}) &= \sqrt{\#\mathcal{L}(d_G, d_G)} \\ &= \frac{1}{d_G!}\sqrt{\frac{n!}{(n-2d_G)!}}\end{aligned}$$

同様に暗号文について総当たりする空間は $\mathcal{L}(d_R, d_R)$ であるので, 暗号文の安全性 (MessageSecurity) は

$$\begin{aligned}(\text{MessageSecurity}) &= \sqrt{\#\mathcal{L}(d_R, d_R)} \\ &= \frac{1}{d_R!}\sqrt{\frac{n!}{(n-2d_R)!}}\end{aligned}$$

である.

4.1.2 MTRU

定理 5 (総当たり攻撃に対する安全性)

MTRU における公開鍵に対する総当たり攻撃の安全性 (KeySecurity) は,

$$\begin{aligned}(\text{KeySecurity}) &= \sqrt{\#\mathcal{L}_P(d_G, d_G)} \\ &= \frac{1}{d_G!}\sqrt{\frac{n_p!}{(n_p-2d_G)!}}\end{aligned}$$

暗号文の安全性は (MessageSecurity) は,

$$\begin{aligned}(\text{MessageSecurity}) &= (\sqrt{\#\mathcal{L}_P(d_R, d_R)})^{l_p} \\ &= \left(\frac{1}{d_R!}\sqrt{\frac{n_p!}{(n_p-2d_R)!}}\right)^{l_p}\end{aligned}$$

である.

証明

公開鍵の作り方は以下であるので, 総当たりする空間は $\mathcal{L}_P(d_G, d_G)$ である.

$$H \equiv G \circledast F_Q^{-1} \qquad (\text{mod } q)(\text{mod } Q)$$

よって, 安全性は公開鍵の安全性 (KeySecurity) は

$$\begin{aligned}(\text{KeySecurity}) &= \sqrt{\#\mathcal{L}_P(d_G, d_G)} \\ &= \sqrt{\binom{n_p}{d_G} * \binom{n_p - d_G}{d_G}} \\ &= \frac{1}{d_G!}\sqrt{\frac{n_p!}{(n_p - 2d_G)!}}\end{aligned}$$

暗号文に対して, 総当たりする空間は $(\mathcal{L}_P(d_R, d_R))$ である. よって暗号文の安全性 (MessageSecurity) は

$$\begin{aligned}(\text{MessageSecurity}) &= (\sqrt{(\#\mathcal{L}_P(d_R, d_R))})^{l_p} \\ &= \left(\sqrt{\binom{n_p}{d_R} * \binom{n_p - d_R}{d_R}}\right)^{l_p} \\ &= \left(\frac{1}{d_R!}\sqrt{\frac{n_p!}{(n_p - 2d_R)!}}\right)^{l_p}\end{aligned}$$

□

4.2 格子簡約攻撃

Coppersmith, Shamir[2] によれば, NTRU 暗号はある格子に対して LLL アルゴリズムにより簡約基底を求め, 公開鍵から秘密鍵と等価な鍵を得ることができる.
公開鍵を

$$H = \sum_{i=0}^{n} h_i x^i$$

として H の係数ベクトルの巡回行列を M_H とする.

$$M_H = \begin{pmatrix} h_0 & h_1 & \cdots & h_{n-1} \\ h_{n-1} & h_0 & \cdots & h_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \cdots & h_0 \end{pmatrix}$$

V_f を f の係数ベクトル, V_g を g の係数ベクトルとして以下のことが成り立つ.

$$V_f M_H = V_g$$

ここで次のような格子を考える. I を (n, n) 単位行列として

$$L_M = \begin{pmatrix} \alpha I & M_H \\ O & qI \end{pmatrix}$$

この簡約基底は整数結合で表されるので F, G と等価な鍵が見つかる.

以下, MTRU において格子簡約攻撃について検討する. M_h は R/I 上の倍行列であるので, R/Q 上の h 倍行列を考えてこれを M'_h とする. このとき, $V_f * M'_h = V_g$ であるので NTRU 格子と同様に格子を構成する. I を (n_q, n_q) 単位行列として

$$L'_M = \begin{pmatrix} \alpha I & M_h \\ O & qI \end{pmatrix}$$

この格子の列ベクトルは $vh \equiv w \pmod q \pmod Q$ を満たす $(\alpha v, w)$ である. NTRU においてはこの簡約基底が $(\alpha V_f, V_g)$ と等価な鍵を含んでいるが, MTRU では L'_M の簡約基底に $(\alpha V_f, V_g)$ と等価な鍵は含まれなかった. よって NTRU に対する格子簡約攻撃をそのまま MTRU に適用することはできない. ただし, 他の格子を用いた LLL アルゴリズムによる攻撃を受ける可能性はある.

5 実装

Risa/Asir[4] を用いて NTRU と MTRU 実装した.
計算機環境は CPU:Intel Corei7 2.8GHz, MEMORY:DDR3 16GB, OS:MacOSX10.6.4,
Risa/Asir:Version 20100526 である.
実験は鍵を生成し, 30KB のテキストデータを暗号化し復号した.

表 1 は NTRU の実験結果であり, n, d_F, d_G, d_R は NTRU[1] で提案されているは 3 つのパラメータの取り方である.p, q は MTRU に合わせた.

表 2 はそれぞれ 2 変数の MTRU の実験結果である. d_F, d_G, d_R は NTRU と同じものとした. グレブナ基底は NTRU を単純に拡張した形の $P = \langle x_1^a - 1, \cdots, x_m^a - 1\rangle, Q = \langle x_1^b - 1, \cdots, x_m^b - 1\rangle$ とした. また a は NTRU と MTRU の KeySecurity をほぼ同じにするようにとった.

key, enc, dec はそれぞれ鍵生成, 暗号化, 復号にかかった時間 (秒) であり, file は暗号文の大きさ (KB) である. ks は KeySecurity, ms は MessageSecurity である.

表 1: NTRU

n	p	q	d_F	d_G	d_R	key	enc	dec	file	ks	ms
107	257	4001	15	12	5	0.0132	5.314	12.01	56	2^{50}	2^{26}
167	257	10007	61	20	18	0.0451	11.43	24.57	56	$2^{82.9}$	2^{77}
503	257	50021	216	72	55	0.4861	32.95	80.38	56	2^{285}	2^{241}

表 2: MTRU(2)

a	b	p	q	d_F	d_G	d_R	key	enc	dec	file	ks	ms
11	31	257	4001	15	12	5	0.522304	21.7948	25.1962	416	2^{52}	2^{54}
13	38	257	10007	61	20	18	1.26893	38.3982	46.0382	458	$2^{83.3}$	2^{167}
23	68	257	50021	216	72	55	34.0335	132.232	171.108	479	2^{291}	2^{582}

参　献

[1] J. Hoffstein, J. Pipher and J. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem" , CRYPTO 1996, Lecture Notes in Computer Science, Vol. 1423, 1998, pp. 267–288.

[2] D. Coppersmith and A. Shamir, "Lattice attacks on NTRU", EUROCRYPT 1997 , Lecture Notes in Computer Science, Vol. 1233, 1997, pp. 52–61.

[3] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRUSIGN:Digital signatures using the NTRU lattice" - CT-RSA 2003 [3-540-00847-0] Hoffstein.

[4] Risa/Asir
http://www.math.kobe-u.ac.jp/Asir/asir-ja.html